

TWO-TIERED AUTHORIZATION AND AUTHENTICATION FOR A CABLE DATA DELIVERY SYSTEM

Cross Reference to Related Application

This is a continuation of U.S. Application No. 08/835,916, filed April 10, 1997, which claimed the benefit of U.S. Provisional Application No. 60/035,618, filed January 17, 1997.

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates to the field of cable data delivery systems and, more particularly, to a two-tiered authorization and authentication system for a cable delivery system.

2. Description of the Relevant Art

In the not-too-distant past, images could be processed and displayed only by large, special-purpose computer systems. Owners of lower-cost and less-powerful computers such as personal computers had to content themselves with character-based displays. The cost of memory has dropped so quickly and the power of microprocessors has increased so greatly in recent years, however,

0929750-09449
F01160-092960

the network where bandwidth is particularly restricted is the analog telephone line that connects most PC users to the Internet.

It has been known for years that the bandwidth of the telephone system can be increased by replacing the analog system with a digital system, but all of the known techniques for doing this require extensive modification of the telephone system.

A great many homes do in fact have a high bandwidth connection, namely that provided by cable television. The problem with this connection is that it is one way. A PC may receive data via a home's CATV cable, but it cannot use the cable to send data. Again, ways of making the CATV system bidirectional have been known for years. For example, in the early 1980's, Scientific-Atlanta, Inc. introduced and marketed a product known as the Model 6404 Broadband Data Modem for use with bidirectional CATV systems.

Scientific-Atlanta, Inc. has also recently filed U.S. Patent Applications Serial Numbers 08/627,062, filed April 3, 1996, 08/738,668, filed October 16, 1996, and a continuation-in-part titled *System and Method for Providing Statistics for Flexible Billing in a Cable Environment*, Koperda, et al., filed March 14, 1997 which describe bidirectional CATV systems. As with the telephone systems, the problem here is not the technology, but the fact that its introduction requires extensive modification of most existing CATV systems.

Given that many homes have a CATV cable and virtually all homes have an analog telephone line, systems have been proposed in which the CATV cable is used to send data from the Internet to the PC and the telephone line used to return data from the PC to the Internet. These systems take advantage of the fact that by far the most common pattern of interaction between users and networks is for the user to retrieve a large amount of data over the network, for example an image of a restored art work from Florence, examine the image, and then send a few keystrokes over the network. With this kind of interaction, far less bandwidth is needed in the channel that is used to return the keystrokes than in the channel that is used to fetch the image.

An example of such a system is the one disclosed in Moura, et al., *Asymmetric Hybrid Access System and Method*, U.S. Patent 5,586,121, issued December 17, 1996, and in Moura, et al., *Remote Link Adapter for use in TV Broadcast Data Transmission System*, U.S. Patent 5,347,304, issued Sept. 13, 1994. In this system, the head end of a cable system has high bandwidth access to the Internet or to other networks and access via CATV cables and the telephone system to households or businesses with PCs. Data received from these networks is sent to PCs connected to the cable system's cables and responses from the PCs are collected via the telephone system and sent to the network. In the home or business, the PC is connected either directly or via a local area network to a

device which includes both a radio frequency modem and a standard analog telephone modem. The radio frequency modem is connected to the CATV cable. It receives and decodes the data sent on the CATV cable and provides it to the PC. The telephone modem is connected to a standard telephone line. It receives data from the PC and sends it to the CATV head end, which in turn forwards it to the Internet or other networks.

While systems such as the one disclosed in the Moura references do provide a solution to the bandwidth problem, they have a number of deficiencies, particularly when used in the context of the Internet. Among the deficiencies are the following:

The system of Moura wastes Internet Protocol (IP) addresses for the computers attached to the modem. IP addresses are in short supply. In the system of Moura, however, IP addresses are statically assigned to the PCs and are consequently not available for reuse when a PC is idle or not engaged in an activity which involves network access.

From the point of view of the Internet, the system of Moura is a link level system, that is, the components of the system of Moura do not themselves have IP addresses and cannot themselves execute IP protocols. In particular, IP routing is not used within the system of Moura. One difficulty arising from this situation is that IP routing is centralized in the IP router that connects the

head end to the Internet; another is that the modem in the system of Moura cannot function as an IP router.

In Moura, the telephone connection to the modem is used solely to transfer data from the PC and modem to the head end. All data received by the PC and modem is sent via the CATV cable. Consequently, when the CATV system fails, the PC is left without a connection by which it can receive data. This situation is made even less desirable by the fact that CATV systems are far more likely to fail than the telephone system.

The CATV channel to which the modem of Moura responds is statically assigned to a given modem, thereby rendering the channel unavailable for use by other modems when the PC connected to the given modem is idle or is not engaged in an activity which involves network access.

The Moura system is further deficient in that it does not have adequate provisions for preventing unauthorized use of the system. Thus, the system is subject to revenue loss for the system provider. Such losses result in an overall increase in the operating cost of the system, which ultimately must be passed on to the authorized subscribers.

Accordingly, there is a great need for a system like the one disclosed by Moura, but which is not burdened by the aforementioned deficiencies.

SUMMARY OF THE INVENTION

In accordance with the principles of the present invention, there is provided a cable data delivery system in which the downstream data delivery system is provided over an existing cable television distribution network and the upstream path from a subscriber is provided over a standard telephone line. A special modem, described below, is used to interface the upstream and downstream paths.

In accordance with the invention, a subscriber uses the modem to log onto the system over the upstream path using a USERID and password. The system then validates this information with a stored database of valid USERIDs and associated passwords. After the USERID and password are validated, the modem then initiates an interaction with the system control server over the upstream telephone path. During this interaction, the modem sends its electronic serial number to the control server for validation along with a request for the system to allocate system resources so that the modem can receive high data rate transmissions over the cable television distribution system downstream path. The modem's electronic serial number is also compared with a stored database of valid serial numbers for validation. The subscriber will not be authorized to use the entire system unless the USERID, password and modem serial number are shown to be valid for the particular user.

Thus, the system of the present invention provides two tiers of authorization and authentication. The first tier, validation of the subscriber's USERID and password, are required for the subscriber to establish the initial telephone connection with the system. In one embodiment of applicant's system, establishment of the initial telephone connection over the telephone line is sufficient for the user to conduct, for example, an Internet session as is currently done in the prior art with a conventional modem and a convention telephone connection. This level of service does not, however, utilize the full features of Application's invention with respect to providing high data rates back to the subscriber over the cable television network. The higher level of service requires the second tier of authorization involving the validation of the electronic serial number.

The two tier authorization and authentication approach employed in the present invention results in a significant level of security for the system, thus preventing unauthorized use of the system and the resulting loss in revenue for the system provider. Needless to say, resulting losses due to unauthorized use of the system ultimately results in higher cost for the subscriber as well.

Further details and features of the present invention will be understood from reading the detailed description of the invention in view of the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is an overview of the physical components of the cable data network disclosed herein;

Figure 2 shows the channels, superframes, and superpackets used to carry data on the RF link in the preferred embodiment;

Figure 3 is a block diagram of a preferred embodiment of the RF modem employed in the cable data network; and

Figure 4 is a diagram that shows how the RF modem receives IP addresses and a <channel,pipe,link ID> triple when the RF modem becomes active.

BRIEF DESCRIPTION OF THE PREFERRED EMBODIMENT

Figure 1 shows the physical components of cable data network 100 in a preferred embodiment. Cable data network 100 transfers data packets with IP addresses between Internet 150 and hosts 108, which in a preferred embodiment are PCs or work stations. Cable data network 100 also transfers packets with IP (Internet Protocol) addresses among the components of cable data network 100 and uses Internet 150 to exchange data packets with IP addresses between cable data network 100 and remotely-located control and management components 111. These components typically deal with functions such as receiving information about new subscribers or billing.

In a preferred embodiment, cable data network 100 is implemented in a cable television (CATV) system. Packets from Internet 150 that contain the IP address of a host 108(i) are

received in CATV head end 122, are put in the proper form for transmittal over cable 132 belonging to the CATV system, and are transmitted via cable 132 to RF modem 106(j) to which destination host 108 (i) is attached. RF modem 106(j) reads the IP address of host 108 from the packet and routes the packet to host 108(i). Packets from host 108(i) which are intended for a destination in Internet 150 go to RF modem 106(j), which routes them via telephone line 131 and public switched telephone network (PSTN) 109 to a telephone modem (Tmodem) 110(k) in telephone modem pool 135 in head end 122. Tmodem 110(k) routes the packet to router 101, which routes it to Internet 150. Since public switched telephone network 109 allows bidirectional communication, router 101 may also route packets received from Internet 150 for host 108(i) to host 108(i) via tmodem 110(k) and RF modem 106(j). As will be explained in more detail in the following, this route is used in the event of a failure in the CATV portion of network 100.

Continuing with the details of the implementation of cable data network 100, data packets are transferred between Internet 150 and CATV head end 122 by means of a transmission medium belonging to a wide-area backbone network 124. Typically, the transmission medium will be a high-speed, high-capacity fiber optic cable such as a T1 or T3 cable, but it could also be a terrestrial or satellite microwave link. The transmission medium is connected to router 101, which in a preferred embodiment may be a router

belonging to the 7000 series manufactured by Cisco Systems, Inc., San Jose, CA.

Router 101 is coupled between WAN backbone 124 and local-area network (LAN) 120, which is the link-level network that connects the components of cable data network 100 which are located in CATV head end 122. Router 101 may both receive packets from backbone 124 or LAN 120 and provide them to backbone 124 or LAN 120. Each component connected to LAN 120 has both an IP address and a LAN address on LAN 120, and router 101 contains a routing table which it uses to route IP packets to IP hosts, including other routers.

Router 101 examines every packet it receives on WAN backbone 124 or LAN 120; if the packet's destination IP address is one of the ones in the routing table, router 101 routes it to the component on LAN 120 which is to receive IP packets having that address; if it is not one of the addresses in the routing table, router 101 routes it to WAN backbone 124, which takes it to Internet 150. In each case, router 101 puts the data packet into the proper form to be transmitted via the relevant link-level network.

As will be apparent from the foregoing discussion, LAN 120 and router 101 can be used to route IP packets received from Internet 150 and destined to a host 108 via two routes. The first is via communications manager 102 and cable plant 105, cable 132, and RF modem 106. The second is to host 108 via telephone modem pool 135 and RF modem 106. Packets from host 108 and from RF modem 106 go

currently has an IP address assigned to it. Using the information in the routing table, communications manager 102 makes superframes 405 for each channel 403(i) in the network containing cable 132 . The superframes contain superpackets 407 directed to the RF modems 106 connected to that channel for which communications manager 102 has received IP packets 301. The superframes are stored in a dual-ported memory which is accessible to QPR modulators 103.

There is a QPR modulator 103 for each channel 403 in a given network, and the QPR modulator reads the superframes for its channel, digitally modulates the RF signal for the channel according to the contents of the superframes, and outputs the modulated signal to combiner 104, which combines the outputs from all QPR modulators and provides the combined output to cable plant 105, which outputs it to cables 132 belonging to the network. The QPR modulators employ quadrature partial response modulation. Of course, any kind of digital RF frequency modulation could be employed as well. It should also be pointed out that any arrangement could be employed which relates a given RF modem 106 to a portion of the bandwidth of the network to which cable 132 belongs, rather than the <channel,pipe,LinkID> triple used in the preferred embodiment, and that the portion of the bandwidth that carries packets addressed to hosts 108 connected to a given RF modem 106 can be termed in a broad sense the RF modem's "channel".

Following cable 132 to RF modem 106, RF modem 106 is connected

between cable 132, a LAN 133 to which one or more hosts 108 are connected, and telephone line 131 and provides interfaces to cable 132, LAN 133, and telephone line 131.

Figure 3 shows a block diagram of a preferred embodiment of RF modem 106. The components of RF modem 106 operate under control of CPU 505 and read data from and write data to memory 507, which has three kinds of memory components: static RAM 509, which is nonvolatile, that is, it is writable but retains its contents when RF modem 106 is turned off, dynamic RAM 511, which is volatile, and FLASH RAM 513, which is nonvolatile and writable but will only permit a fixed number of writes. SRAM 509 is used to store data which changes but must be kept across activations of RF modem 106. Examples of such data are the RF modem's telephone number and the addresses of RF modem 106 and hosts 108 on LAN 133. DRAM 511 is used for data that is only valid during an activation, such as the current routing table. FLASH RAM 513 is used for information that changes only rarely, such as the programs executed by CPU 505. In the preferred embodiment, RF modem 106 can load programs it receives in IP packets via telephone line 131 into Flash RAM 513.

Turning to the interfaces and beginning with the interface to cable 132, that interface has two main components, tuner 501 and decoder 503. Tuner 501 can be tuned under control of CPU 505 to a channel 403(i) in cable 132. Tuner 501 further demodulates the superframes 405 it receives on that channel and passes them to

decoder 503. Decoder 503 examines superpacket 407(i) for the pipe which carries data addressed to RF modem 106, and if LinkID 413 in superpacket 407(i) specifies RF modem 106, decoder 503 does error correction, decodes the data, and passes it to memory 507. When an IP packet has accumulated in memory 507, CPU 505 examines the destination IP address in the packet, and uses a routing table in memory 507 to determine whether the packet is addressed to a host 108 connected to RF modem 106. If the packet is so addressed, CPU 505 obtains the LAN address corresponding to the IP address. CPU 505 provides the LAN address and the location of the packet in memory 507 to Ethernet integrated circuit 515, which packages the packet into one or more Ethernet frames and outputs it to Ethernet 133.

RF modem may also receive IP packets via phone line 131 and modem chip 517 that are addressed either to the RF modem 106 itself or to one of the hosts 108 connected to RF modem 106. In the first case, RF modem 106 responds to the packet; in the second, it routes the packet to the host as just described for packets from cable 132. When RF modem 106 receives a packet via LAN 133 that is not addressed to RF modem 106 itself, it routes the packet via modem chip 517 and telephone line 131. Included in host 108 is the software 107 necessary to interact with RF modem 106.

Continuing with the portion of the link level that is implemented using the public switched telephone network, modem chip

517 in RF modem 106 is connected by means of a standard analog telephone line 131 to public switched telephone network 109, and RF modem 106 can thus call other telephone numbers via PSTN 109 and be called from other telephone numbers in PSTN 109. In the present case, when RF modem 106 wishes to set up a session that will permit it to transfer IP packets 301 for a host 108, it calls a telephone number for telephone modem pool 135. The modem pool responds by assigning a telephone modem (Tmodem) 110 to RF modem 106 and assigning RF modem 106 an IP address. As shown in FIG. 1, telephone modem pool 135 is also connected to LAN 120 in head end 122. Telephone modem pool 135 serves as a router with respect to LAN 120 and the telephone connections currently being served as by the tmodems 110 in the modem pool. Once a telephone modem 110 and an IP address have been assigned to RF modem 106, RF modem 106 may send IP packets 301 to the devices connected to LAN 120 and receive IP packets 301 from those devices.

As will be explained in more detail in the following, the fact that PSTN 109 provides a bi-directional link between the devices connected to LAN 120 and RF modem 106 is employed to determine where RF modem 106 is in the cable network managed by head end 122, to dynamically assign a <channel,pipe,LinkID> triple in cable 132 to RF modem 106, and to provide an alternate route to hosts 108 connected to RF modem 106 when there is a failure in the RF link between head end 122 and RF modem 106.

The remaining device which is connected to LAN 120 is control/management server 125, which in a preferred embodiment is implemented in software executing on a server constructed by SUN Microsystems, Inc., Mountain View, CA. Control/management server 125 manages CDN 100. It responds to DHCP packets by dynamically allocating IP addresses to hosts 108 and sending SNMP packets to router 101 and communication manager 102 which cause them to set their routing tables as required for the newly-assigned IP addresses, responds to SNMP trap packets from the devices connected to LAN 120 and from FR modems 106, responds to RIP packets as required to update routings, and maintains the Management Information Database used by the SNMP protocol as well as a list of unassigned IP addresses. A graphical user interface in control/management server 125 shows the current status of CDN 100 and permits operator intervention in the operation of cable data network 100.

The structure of an IP packet, IP address routing architecture and addressing architecture of CDN 100 are described in U.S. Application Serial Nos. 08/833,198, filed April 14, 1997; 08/837,073, filed April 11, 1997; U.S. Patent No. 6,208,656, filed April 11, 1997; U.S. Patent No. 6,178,455, filed April 11, 1997; U.S. Application Serial Nos. 08/838,833, filed April 11, 1997; 08/832,714, filed April 11, 1997 and U.S. Patent No. 6/249,523 filed April 11, 1997 and are incorporated herein by reference. These applications will be collectively referred to hereafter as the "incorporated applications." In addition, details on IP addressing and the

also dynamic, i.e., what IP addresses correspond to a given <channel,pipe,link ID> triple is decided only when the IP addresses and the <channel,pipe,link ID> triple are assigned.

A more detailed description of dynamic assignment of IP addresses can be found in the incorporated applications.

Figure 4 shows the interactions 701 between the components of cable data network 100 when a RF modem 106(i) is inactive and a user of host 108(j) connected to RF modem 106(i) wishes to become connected to Internet 150. The user executes routines in software 107 which cause host 108(j) to send a setup request to RF modem 106(i) at modem 106(i)'s address in LAN 133, as shown at 702. Included in the setup request is authentication information such as a user identification and password and the telephone number of telephone modem pool 135. RF modem 106 responds by first sending a dummy IP address to host 108(j) and then dialing the telephone number. Telephone modem pool 135 responds by setting up a Point-to-Point Protocol (PPP) link via PSTN 109 between RF modem 106 and a tmodem 110(k). Once this is done, RF modem 106 sends the authentication information to modem pool 135, which passes them on to control/management server 125. Control management server 125 then checks the authentication information, and if it is valid, control/management server 125 assigns an IP address in network A 206 to RF modem 106(i). It returns the IP address to RF modem

- An IP address for RF modem 106 in Ethernet 133. As will be explained in more detail below, this IP address is not unique to RF modem 106.
- the subnet mask for the host IP addresses.
- IP addresses in network A 206 for a domain name server, for SNMP agent 1203, for communications manager 102, and for router 101.
- Information about where RF modem 106 can obtain current firmware.
- The <channel,pipe, link ID> triple that has been assigned to RF modem 106.

Telephone modem pool 135 forwards the DHCP response packet to RF modem 106(i) (717) and RF modem 106(i) sets its tuner 501 to listen on the specified frequency and its decoder 503 to read superpackets on the specified pipe when they have the RF modem's link ID.

When RF modem 106(i) next receives a DHCPDISCOVER request from any of the IP hosts 108 attached to LAN 133, it responds with a DHCP OFFER packet that contains one of the IP addresses for the hosts that RF modem 106(i) received by the process described above.

In other embodiments, RF modem 106(i) may further respond to the DHCP OFFER packet 715 by sending an acknowledgment IP packet via PSTN 109 and modem pool 135 to communications manager 102 (719). Communications manager 102 responds to the acknowledgment

by sending an acknowledgment 721 on the cable 132 at the frequency and pipe RF modem 106(i) is listening to. The acknowledgment contains at least RF modem 106(i)'s LinkID. Once RF modem 106(i) receives the acknowledgment, it informs host 108(i) which began the transaction of its new IP address. Host 108(i) then replaces the dummy IP address with the new IP address.

The authorization and authentication process in accordance with the present invention will now be further described with reference again to Figure 1.

When a subscriber wishes to initiate a network session, modem 106 is powered up. Upon power up, the modem performs a set of self tests to verify the hardware. After a successful completion of the self tests, the modem is ready to receive commands from the network access software resident in the PC. The subscriber then launches the network access software which opens a logon dialog box on the PC screen requesting the subscriber's USERID, password and telephone number to dial in order to connect with modem pool 135. Ideally, the subscriber's USERID, password and telephone number will be stored in a configuration file associated with the network access software from an earlier session. Thus, when the logon dialog box is displayed, it may already have this information available for the subscriber to review and update if necessary.

The PC then sends the logon information (USERID, password and telephone number) to the cable modem. The modem then dials modem

appropriate system resources are allocated for modem 106 as described above.

It should be obvious from the above-discussed apparatus embodiment that numerous other variations and modifications of the apparatus of this invention are possible, and such will readily occur to those skilled in the art. Accordingly, the scope of this invention is not to be limited to the embodiment disclosed, but is to include any such embodiments as may be encompassed within the scope of the claims appended hereto.

09462660-09462660